<<密码术的奥秘>>

图书基本信息

书名：<<密码术的奥秘>>

13位ISBN编号：9787560085883

10位ISBN编号：7560085881

出版时间：2009-5

出版时间：外语教研

作者：(英)派珀//墨菲|译者:冯绪宁//袁向东

页数：273

<<密码术的奥秘>>

内容概要

密码的成功破译使得第二次世界大战提前两年结束．而误信密码则让16世纪苏格兰的玛丽女王掉了脑袋．可见密码术对我们的历史产生过极为重大的影响。
然而密码术并非只与战争和间谍相关，它渗透到了人们的日常生活中：自动柜员机、电子邮件、付费电视、网络购物、移动通话等无不涉及加密与解密。
　作为密码术的入门图书，本书没有过多纠缠高深的技术理论，却又较为全面地论述了密码术的发展、分类及其应用等方方面面，其中穿插有大量密码术的使用实例，可以说既能丰富普通读者的密码术知识，也是对数学爱好者和密码爱好者的智力挑战。

作者简介

弗雷德·派珀，1975年起担任伦敦大学数学系教授，1979年开始从事安全领域的工作，1985年成立Codes & Ciphers有限责任公司，提供信息安全领域的咨询服务。
现为伦敦大学皇家霍洛威学院信息安全专业的主任。

<<密码术的奥秘>>

书籍目录

章节摘录

最早的密码实例之一是凯撒密码。
尤利乌斯·凯撒（Julius Caesar）在其作品《高卢战记》中首先介绍了这一密码。
在这种密码中，从A到W的每个字母在加密时用字母表中位于其后三位的那个字母代替，字母X、y、z则分别被替换成A、B和C。
在这里，凯撒对字母进行了3“移位”，但用从1到25中的任何数的移位都能产生类似的效果。
事实上，任一种移位现在通常都视为是使用了凯撒密码。
我们再次用一个图表来解释这种密码。
该图表标示了两个同心环，外面的环可以自由转动。
如果我们从外环的字母A对应于内环的A开始，经2次移位外环的c就到了内环A处，等等。
包括0移位（当然它与26移位是同等的）在内，共有26种移位方式。
就凯撒密码而言，其加密密钥与解密密钥都是用移位数来决定的。
一旦双方同意选定一种移位，那么一个凯撒密码的加密就可以这样来完成了：在内环上找到明文中的每个字母，再将它替换成图中外环上与之对应的那个字母。
而解密时只要实施相反的运作即可。
于是，由该图可知经3移位后明文信息DOG变为GRJ，而密码文FDW的明文则为CAT为了使读者更确信自己理解这个系统，我们列出以下陈述供读者验证：如果是7移位，那么对应于VERY的密文是CLYF；而对于17移位，则对应于JLE的明文是SUN。
在我们所描述的凯撒密码中，加密密钥和解密密钥都等于移位数，但加密和解密的规则是不同的。

版权说明